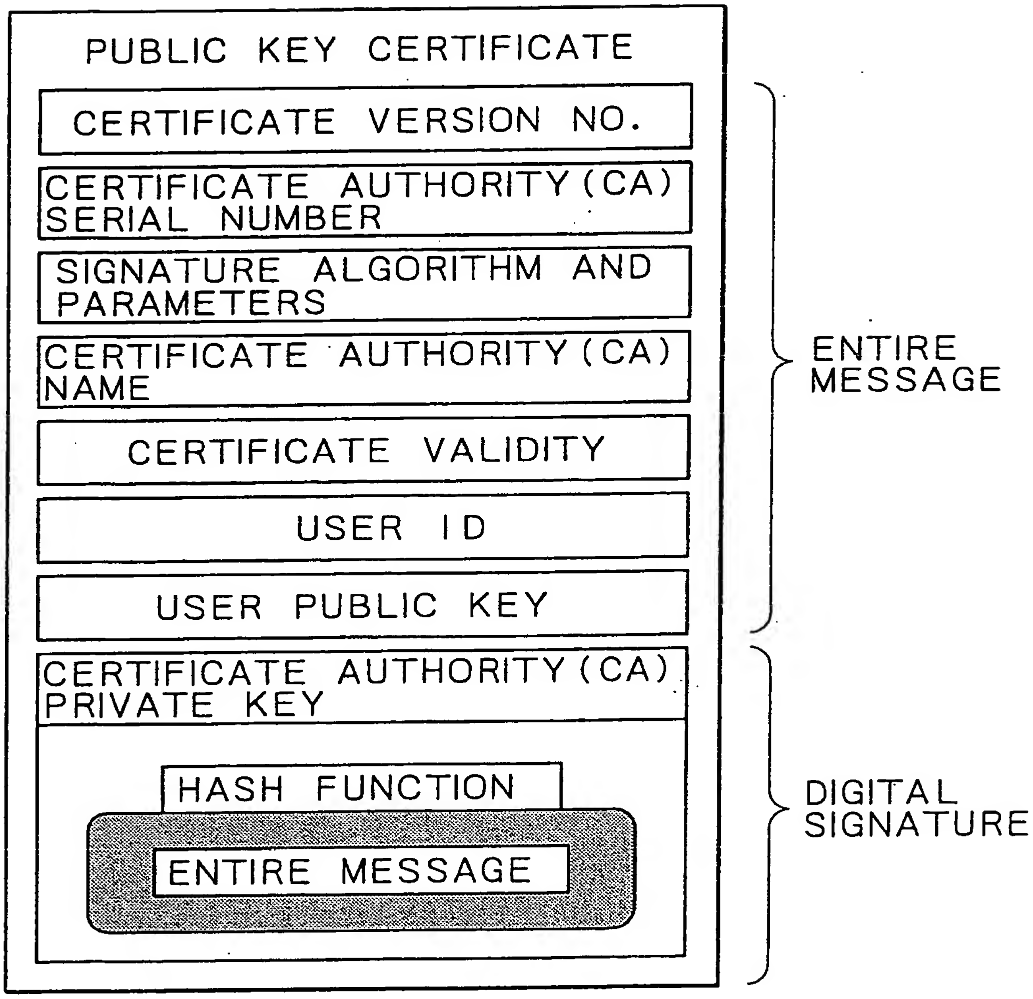
FIG. 1



PRIOR ART

FIG. 21A

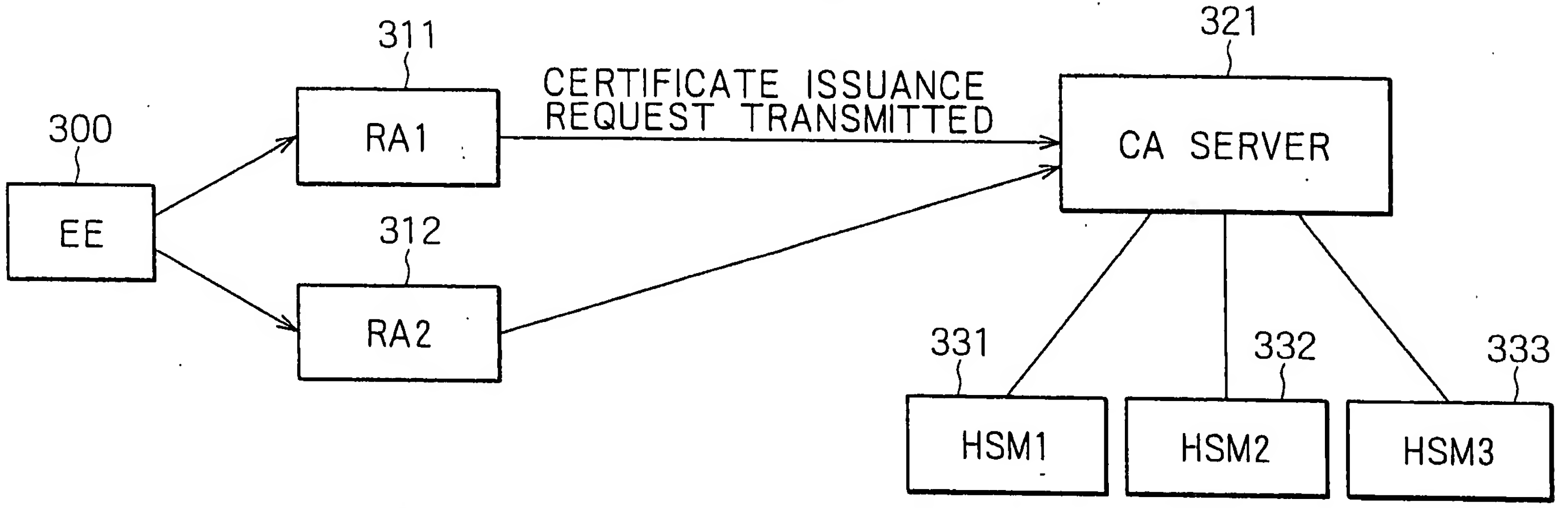


FIG. 21B

RA MANAGEMENT DATABASE

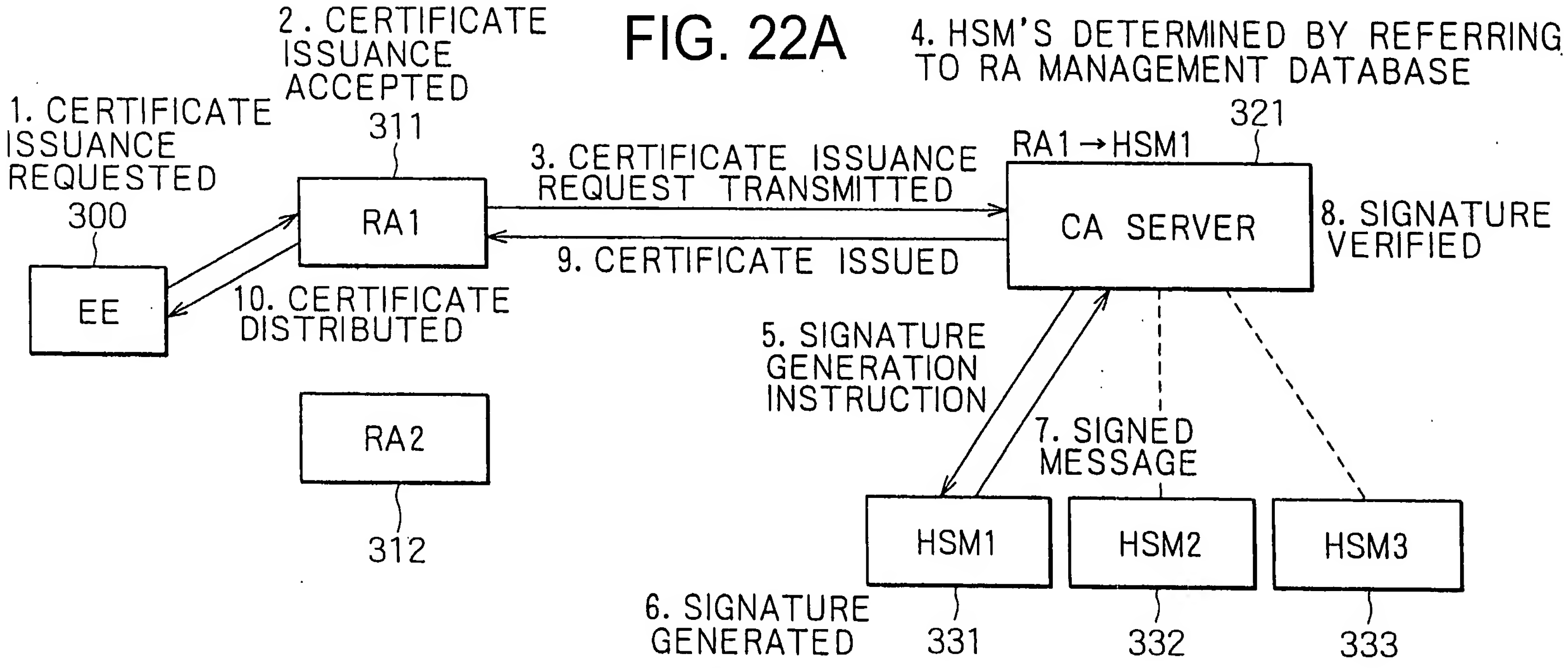
RA ID	USAGE OF MULTIPLE-SIGNATURE ALGORITHM	SIGNATURE ALGORITHM	KEY LENGTH	PARAMETERS	LOAD DISTRIBUTION	HSM IN USE
RA1	×	RSA	1024 bits	–	×	HSM1
RA2	○	RSA	2048 bits	–	×	HSM2
RA2	○	ECDSA	192 bits	p=XX,…	×	HSM3
RA2	○	ECDSA	192 bits	p=YY,…	×	HSM3

FIG. 21C

VERIFICATION KEY DATABASE

HSM ID	SIGNATURE ALGORITHM	KEY LENGTH	PARAMETERS	VERIFICATION KEY
HSM1	RSA	1024 bits	–	◇
HSM2	RSA	2048 bits	–	◆
HSM3	ECDSA	192 bits	p=XX,…	△
HSM3	ECDSA	192 bits	p=YY,…	▲

FIG. 22A


1. CERTIFICATE ISSUANCE REQUESTED
300
EE
2. CERTIFICATE ISSUANCE ACCEPTED
311
RA1
10. CERTIFICATE DISTRIBUTED
RA2
312
3. CERTIFICATE ISSUANCE REQUEST TRANSMITTED
9. CERTIFICATE ISSUED
4. HSM'S DETERMINED BY REFERRING TO RA MANAGEMENT DATABASE
RA1→HSM1
321
CA SERVER
8. SIGNATURE VERIFIED
5. SIGNATURE GENERATION INSTRUCTION
7. SIGNED MESSAGE
6. SIGNATURE GENERATED
HSM1
331
HSM2
332
HSM3
333

CERTIFICATE ISSUANCE REQUEST

COMMAND	MESSAGE	RA ID
CERTIFICATE ISSUANCE	Message1	RA2

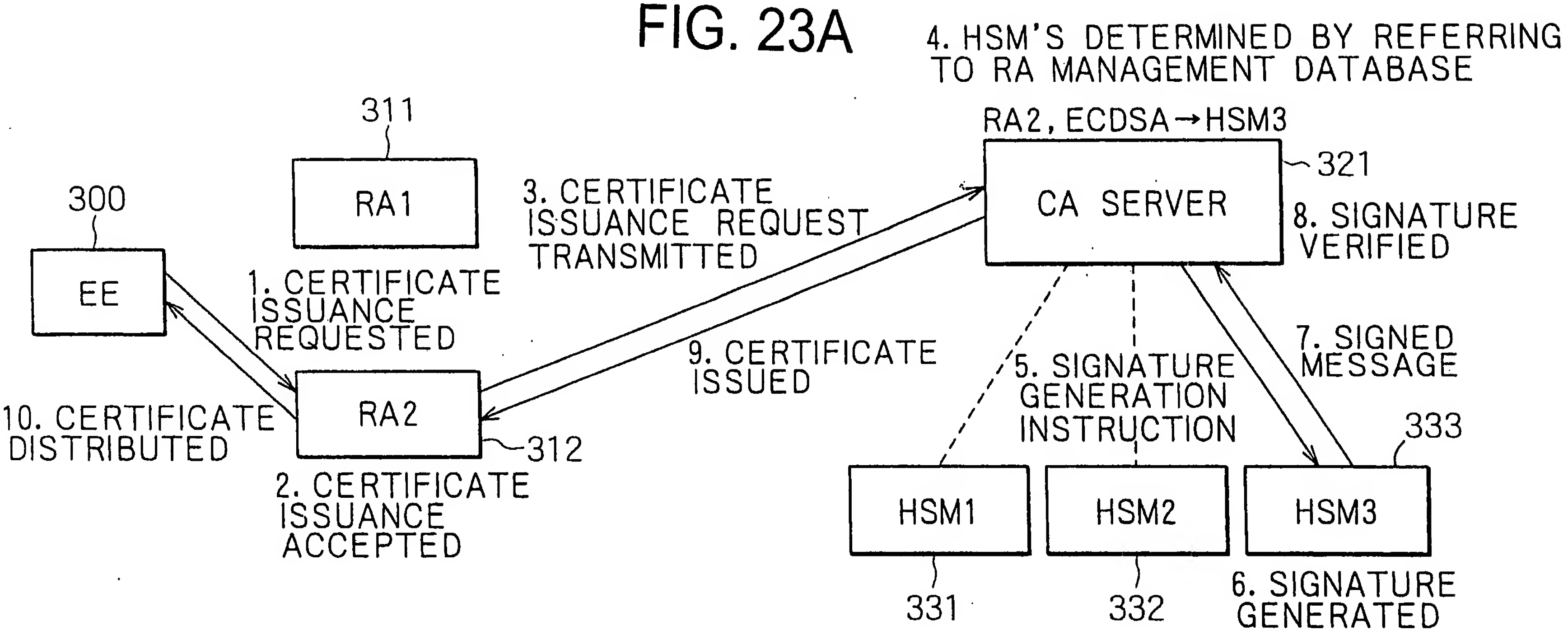
FIG. 22B

SIGNATURE GENERATION INSTRUCTION

COMMAND	MESSAGE
SIGNATURE GENERATION	Message1

FIG. 22C

FIG. 23A


4. HSM'S DETERMINED BY REFERRING TO RA MANAGEMENT DATABASE
RA2, ECDSA→HSM3
300
EE
311
RA1
RA2
312
CA SERVER
321
1. CERTIFICATE ISSUANCE REQUESTED
2. CERTIFICATE ISSUANCE ACCEPTED
3. CERTIFICATE ISSUANCE REQUEST TRANSMITTED
5. SIGNATURE GENERATION INSTRUCTION
6. SIGNATURE GENERATED
7. SIGNED MESSAGE
8. SIGNATURE VERIFIED
9. CERTIFICATE ISSUED
10. CERTIFICATE DISTRIBUTED
HSM1
331
HSM2
332
HSM3
333

CERTIFICATE ISSUANCE REQUEST

COMMAND	MESSAGE	RA ID	SIGNAL ALGORITHM	KEY LENGTH	PARAMETERS
CERTIFICATE ISSUANCE	Message2	RA2	ECDSA	192 bits	p=XX,…

FIG. 23B

SIGNATURE GENERATION INSTRUCTION

COMMAND	MESSAGE	KEY LENGTH	PARAMETERS
SIGNATURE GENERATION	Message2	192 bits	p=XX,…

FIG. 23C

FIG. 24 A

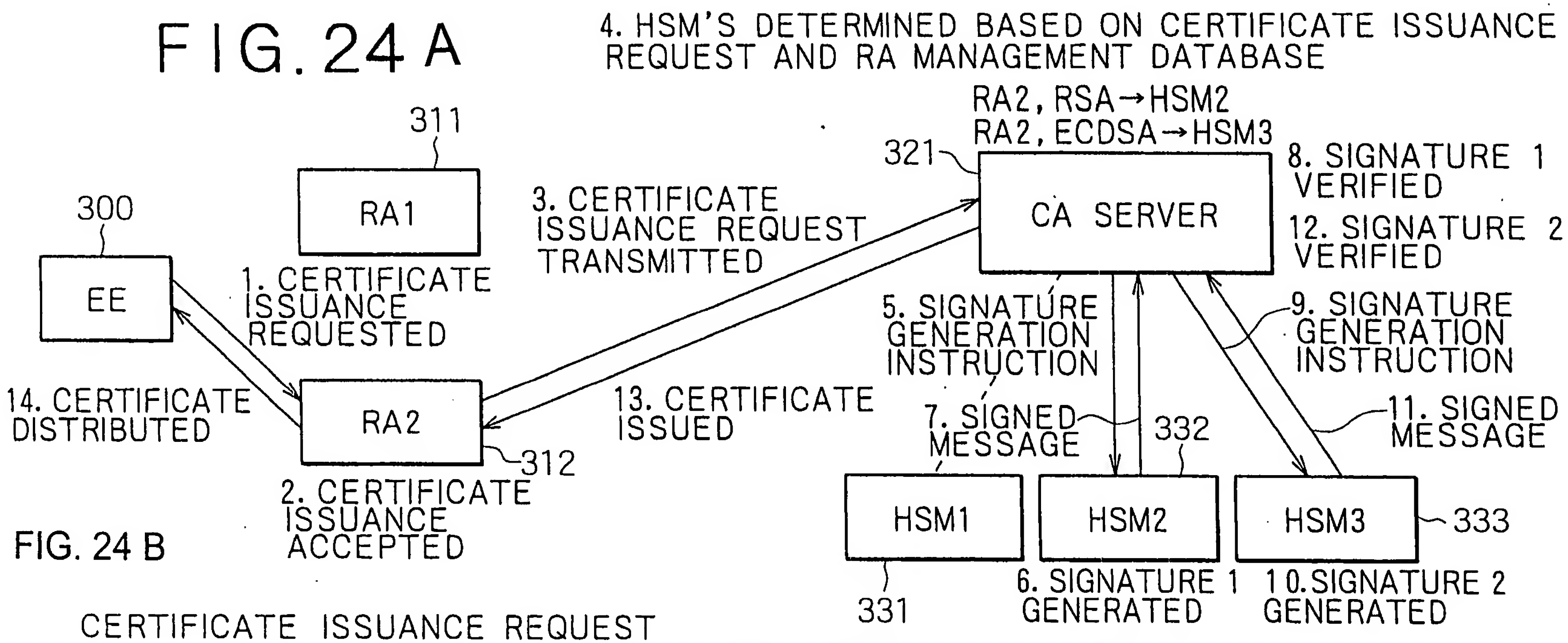

4. HSM'S DETERMINED BASED ON CERTIFICATE ISSUANCE REQUEST AND RA MANAGEMENT DATABASE
RA2, RSA→HSM2
RA2, ECDSA→HSM3
300
EE
311
RA1
1. CERTIFICATE ISSUANCE REQUESTED
14. CERTIFICATE DISTRIBUTED
RA2
312
2. CERTIFICATE ISSUANCE ACCEPTED
3. CERTIFICATE ISSUANCE REQUEST TRANSMITTED
13. CERTIFICATE ISSUED
321
CA SERVER
8. SIGNATURE 1 VERIFIED
12. SIGNATURE 2 VERIFIED
5. SIGNATURE GENERATION INSTRUCTION
7. SIGNED MESSAGE
332
9. SIGNATURE GENERATION INSTRUCTION
11. SIGNED MESSAGE
HSM1
HSM2
HSM3
333
331
6. SIGNATURE 1 GENERATED
10. SIGNATURE 2 GENERATED

FIG. 24 B

CERTIFICATE ISSUANCE REQUEST

COMMAND	MESSAGE	RA ID	SIGNATURE ALGORITHM 1	KEY LENGTH	SIGNATURE ALGORITHM 2	KEY LENGTH	PARAMETERS
CERTIFICATE ISSUANCE	Message3	RA2	RSA	2048 bits	ECDSA	192 bits	p=XX,...

SIGNATURE GENERATION INSTRUCTION

COMMAND	MESSAGE	KEY LENGTH
SIGNATURE GENERATION	Message3	2048 bits

FIG. 24 C

SIGNATURE GENERATION INSTRUCTION

COMMAND	MESSAGE	KEY LENGTH	PARAMETERS
SIGNATURE GENERATION	Message3	192 bits	p=YY,...

FIG. 24 D